DEPARTMENT OF DEFENSE • DEFENSE SECURITY SERVICE, DIRECTORATE FOR SECURITY PROGRAMS

INDUSTRIAL SECURITY LETTER

Industrial Security letters will be issued periodically to inform Industry, User Agencies and DoD Activities of developments relating to industrial security. The contents of these letters are for information and clarification of existing policy and requirements. Local reproduction of these letters in their original form for the internal use of addressees is authorized. Suggestions and articles for inclusion in the Letter will be appreciated. Articles and ideas contributed will become the property of DSS. Contractor requests for copies of the Letter and inquires concerning specific information should be addressed to the cognizant security office, for referral to the Directorate for Security Programs, Headquarters, DSS, as appropriate.

ISL 01L-1 **February 13, 2001**

This is a special section of the Industrial Security Letter (ISL) dedicated to interpreting and clarifying the May 1, 2000 Chapter 8. The document compliments the Director of Central Intelligence Directive (DCID 6/3) "Protecting Sensitive Compartmented Information within Information Systems." The ISL provides industry with the DoD perspective on protecting classified information while maintaining uniformity and consistency with established Department of Defense (DoD) policies. There are references to additional technical data or information being present on the DSS website (www.dss.mil) in the responses to a number of questions in this ISL. That additional information will be posted on March 9, 2001.

Change 2 to the NISPOM, which was approved on May 1, 2000, is attached and can also be found on the Defense Security Service website at www.dss.mil/isec/nispom_change_2.htm. There are 4 revisions included in this NISPOM change: (1) The elimination of contractor-granted Confidential clearances by January 1, 2004; (2) The requirement to retain a signed copy of an electronically submitted personnel security questionnaire; (3) The elimination of non-GSA approved security containers for the storage of Secret information by October 1, 2012; and (4) A total rewrite of Chapter 8, Information Systems Security.

1. Question: What is the implementation date of the May 1, 2000 Chapter 8?

Answer: The implementation date is May 1, 2001. All Information Systems (IS) submitted for accreditation or reaccreditation after this date shall implement the requirements of the new chapter.

2. Question: Will Automated Information Systems (AIS) accredited under Chapter 8 of the 1995 NISPOM retain their accreditation?

Answer: Yes. Currently accredited AISs retain their accreditation for three years from May 1, 2001. Within the three-year period, contractors shall implement the requirements of the new chapter and request reaccreditation for all IS accredited against the 1995 Chapter 8 requirements.

3. Question: When will training become available for the new Chapter 8?

Answer: The DSS Academy has prepared a presentation describing the changes between the January 1995 and May 2000 version of the NISPOM chapter 8. This presentation is annotated so that contractor personnel can provide training within their own organizations. The presentation can be viewed at, or downloaded from, **www.dss.mil/infoas/index.htm**. For a more in-depth class of Information Security that includes the new Chapter 8, the DSS Academy has updated the IS Security Procedures for Industry Course. The course will be available beginning February 2001. The Central Intelligence Agency has also developed training for DCID 6/3. DSS will post information on that and any additional available training.

4. Question: Paragraph 8-100a states that the IS must be properly managed to protect against loss of data integrity and to ensure the availability of the data and system. Paragraph 8-400 states that integrity and availability are not covered by the National Industrial Security Program (NISP) and will be determined in additional guidance or requirements issued by the GCA. Is paragraph 8-100a addressing "general security concerns" and not National Industrial Security Program Operating Manual (NISPOM) requirements?

Answer: Yes. While important, data integrity and system availability are not covered by the NISP (paragraph 8-400) and will be determined in additional guidance or requirements issued by the GCA.

5. Question: Paragraph 8-100c states that "additional requirements for high-risk systems and data are covered in the NISPOM supplement. What is the definition of "high-risk systems and data?"

Answer: "High-risk" refers to the vulnerability and the nature of the technology, process, or data relative to other classified systems and data. For the purpose of this ISL, a high-risk system is one that requires protection above the baseline of chapter 8 (i.e., multilevel) where high-risk data would be non-collateral data. *NOTE: Director of Central Intelligence Directive (DCID) 6/3 is being coordinated as Chapter 8 of the NISPOM Supplement (Automated Information System Security). The requirements of Protection Level 4 of the DCID 6/3 should be used for "high risk" systems and data. These requirements can be found at* ***www.dss.mil/infoas/index.htm.***

6. Question: Paragraph 8-101a. Will a copy of the risk management evaluation be given to the contractor?

Answer: In many facilities the level of complexity of the contractor's IS program or the sensitivity of their classified projects does not warrant a "formal" risk management evaluation and report. When one is required, the Facility Security Officer (FSO) and Information System Security Manager (ISSM) will be provided a copy.

7. Question: Paragraph 8-101b. Must the ISSM be an employee of the contractor and can an ISSM manage the IS security program for more than one contractor?

Answer: The ISSM must be an employee. However, in a multiple facility organization, contractor management can appoint an employee as the ISSM with oversight responsibility for multiple facilities. The travel distance between these facilities should not be greater than one hour, the complexity of any one, or all, facilities is such that only one ISSM is required, the ISSM is trained to a level commensurate with the overall complexity of all facilities, and that each facility has an appointed Information System Security Officer(s) (ISSO) that has been assigned all responsibilities identified in paragraph 8-104.

8. Question: Paragraph 8-101b. What training should the ISSM receive and how will management assure the requirement is met?

Answer: Contractor management should take maximum advantage of the DSS IS for Industry Course to train the ISSM. The course is offered in various locations around the country approximately 12 times a year. The ISSM can also arrange to take any nationally known or government agency information system security training which includes testing or certification.

9. Question: Paragraph 8-102 states the CSA is the Designated Accrediting/Approving Authority (DAA) responsible for accrediting IS used to process classified information. Since this is the first time the NISPOM has identified this position and responsibility, would you elaborate?

Answer: Within the NISP, the Designated Approving Authority (DAA) is the government official with the authority to formally accredit operation of the contractor's IS. Officially the DAA declares the environment the contractor has identified in their System Security Plan (SSP) will effectively protect classified information from unauthorized disclosure. The DAA provides a level of assurance that the IS will provide the protection required. As a general rule, the DSS Industrial Security Representative (IS Rep) assigned responsibility for the contractor's facility is the DAA for standalone IS. The DAA for all other IS will be the DSS regional IS manager.

10. Question: Paragraph 8-103f(5). When is it "appropriate" to implement security features for the detection of malicious code and viruses?

Answer: As a general rule, malicious code and viruses are a concern to all IS and must be addressed by the ISSM and identified in the SSP. However, there are special categories of IS (Section 5) that are immune to these threats and do not require detection procedures.

11. Question: Paragraph 8-104d requires an IS certification test be developed and implemented. What is a certification test and when would it be required?

Answer: A certification test outlines the inspection and test procedures used to demonstrate compliance with the security requirements associated with the Protection Level assigned to the IS. The certification test is administered during the certification process and is discussed later (paragraph 8-614) in this ISL.

12. Question: Paragraph 8-104g(1). When is it "applicable" for each IS to be covered by the facility Configuration Management (CM) program?

Answer: The CM program varies with the complexity and size of the IS. Some IS require a formal configuration management board that makes change control decisions where others might require only the coordination and approval of the ISSO. Every SSP must have a CM section describing how the accredited IS protection features are implemented and maintained.

13. Question: Paragraphs 8-104l and 8-303g require that active user Ids be revalidated at least annually. Is there a requirement to revalidate users of standalone workstations or small local area networks (paragraph 8-303c) since user Ids are not required?

Answer: Yes. The intent of this paragraph is to verify that all users have a continued need to access the accredited IS. Since user Ids are not always required (paragraph 8-303c), access lists can be used. If used for revalidation, access lists shall be retained as an Audit 1 requirement.

14. Issue: Section 2 identifies the requirements associated with the certification and accreditation process. Certification is the comprehensive analysis to validate both technical and nontechnical security features and safeguards of the IS and is conducted in support of the accreditation process. In December 1997, the Office of the Secretary of Defense signed a directive that implements a standard infrastructure-centric approach to the certification and accreditation process. The DoD Information Technology Security Certification and Accreditation Process (DITSCAP) implements policy, assigns responsibility and prescribes procedures to all DoD Agencies, their contractors and agents. The DITSCAP can only be imposed via a requirements clause in the contract. Since the DITSCAP is a process that focuses mainly on government certifiers and accreditors, the DITSCAP has little impact on the contractor other than requiring a System Security Authorization Agreement (SSAA) that is prepared and updated during the lifecycle of the IS. Where the DITSCAP is imposed by contract or otherwise adopted by a contractor under the terms of its GCA's security requirements, the contractor has the option of maintaining the SSAA and the System Security Plan (SSP) separately or of using the DSS modified SSAA that combines both into one document **(www.dss.mil/infoas/index.htm).**

15. Question: Paragraph 8-201 introduces a new requirement of the ISSM certifying that their ISs have undergone a comprehensive evaluation of all technical and non-technical security features and safeguards. Is this all that is required for certification?

Answer: No. DSS is assigned the responsibility of certification (paragraph 8-101). DSS has implemented an internal process of certifying contractor's IS that their IS Reps and ISSPs follow. Part of this process includes the ISSM certifying that their ISs have undergone a comprehensive evaluation.

16. Question: Paragraph 8-202a permits a contractor's IS to be granted interim approval to operate for 180 days with an optional extension of a second 180 days. Under what conditions would an IS require an interim approval of up to 360 days?

Answer: Interim approvals that last up to 360 days should be rare. Normally, interim approvals are granted by the DAA so the contractor can begin processing classified information while the DAA is reviewing the contractor's IS during the accreditation process. Interim approvals must be in writing and must identify what protection measures are required.

17. Question: Paragraph 8-202c. Which procedures should the contractor follow when reviewing changes to security-relevant resources?

Answer: The contractor's configuration management (CM) program will address the review and approval process of security-relevant resources and changes. Additionally, the CM program will identify that DSS must be notified prior to the changes being implemented so a reaccreditation decision can be made.

18. Question: Paragraph 8-202d. Who is responsible for re-evaluating the IS, tracking the 3 year suspense, and what notification to DSS is required?

Answer: It is the ISSM's responsibility to re-evaluate each IS for changes that would require reaccreditation (paragraph 8-202b). If no changes were made, the ISSM would notify DSS by phone, postal or electronic mail. After verifying the original accreditation was valid, DSS would annotate the original accreditation letter with the date of the re-evaluation and provide a copy to the ISSM.

19. Issue: Paragraph 8-202f introduces a new concept of "invalidation" without identifying how, or if, this is different from withdrawal of accreditation (8-202e).

Answer: The end result for either withdrawal or invalidation is the same, the IS is not authorized to process classified information. The difference is in the process and the extent that classified information might be compromised. Invalidation by the DAA requires immediate termination of classified processing. Invalidation is caused when "detrimental" security-significant changes occur that could cause a compromise of classified information. Withdrawal requires the DAA to evaluate new or different risks. During the evaluation, the DAA may decide to permit classified processing to continue.

20. Question: Paragraph 8-202g. Can a multiple facility organization develop just one master SSP covering all locations?

Answer: No. Each facility is responsible for developing and maintaining their own master SSP.

21. Question: Paragraph 8-202g. Can "one" master SSP be written that covers all IS within the contractor's facility that operates at Protection Levels 1 and 2?

Answer: No. A master SSP can be prepared for "similar" IS that operate in equivalent operational environments (i.e., a master SSP for stand alone workstations, another for multi-user IS or local networks).

22. Question: Paragraph 8-202g(3) requires the ISSM to certify additional ISs under a master SSP but does not require notification to DSS. Should DSS be notified?

Answer: Yes. The number of accredited ISs and SSPs are used in determining the size and complexity of the contractor's security program.

23. Question: Paragraph 8-301. Where can instructions on clearing and sanitizing IS memory and media be found?

Answer: DSS posted the clearing and sanitization matrix at **<u>www.dss.mil/infoas/index.htm</u>** along with instructions/procedures on their use.

24. Question: Paragraph - 8-301a provides the requirements for clearing data from memory and media. When is "clearing" required?

Answer: Clearing of memory and media is required (sanitized for TOP SECRET) before and after periods processing (paragraph 8-502a) and as a method of ensuring need-to-know protection, and prior to maintenance (paragraph 8-304b(3).

25. Question: Paragraph 8-302a. What are the review requirements of contractors that develop unclassified software that will be used during classified processing periods?

Answer: Unclassified software, that will eventually be used during classified processing periods, is either developed by cleared, knowledgeable personnel or reviewed and/or tested by cleared, knowledgeable personnel. The review and/or testing is to provide reasonable assurance that security vulnerabilities do not exist.

26. Question: Paragraph 8-302a. Are contractor employees that test commercially procured or security-related software required to have a clearance?

Answer: Yes. By definition, they are "privileged users" as per paragraph 8-105a and require a security clearance to the level the IS is accredited.

27. Question: Paragraph 8-302a. Can commercially procured or security related software be used to configure (e.g. disconnect hardware components not used for classified processing) the IS for a classified processing session?

Answer: Yes. Provided the IS is not accredited TOP SECRET.

28. Question: Paragraph 8-303c permits physical security controls and personnel security controls to augment the logon authentication requirement for standalone workstations or local area networks. What types of personnel security controls are acceptable?

Answer: The ISSM/ISSO are responsible for verifying all users' clearance and need-to-know requirements. Once briefed, the users' names will be added to the area access list or the equipment authorization lists which authenticates that the user is authorized and briefed. The access lists shall be retained as an Audit 1 requirement.

29. Question: Paragraph 8-303c permits physical security and personnel security controls in place of logon authenticators for small local area networks. Does “small” refer to the number of workstations or the area in which the workstations reside?

Answer: The area, to include size, in which the workstations are located. Paragraph 8-303 is addressing an alternative authentication procedure where the ISSO will be able to quickly and easily authenticate the users.

30. Question: Paragraph 8-303i(3). What method(s) of password generation will DSS approve?

Answer: The preferred method of password generation is for the IS to generate unique, random passwords. However, users are permitted to generate their own passwords. User generated passwords must be a minimum of eight alpha/numeric upper/lower case characters. Users shall be briefed not to use dictionary definable passwords to include sport names, pets or family members. The SSP must address the password generation method (i.e., IS or user generated), length and whether the password is unique and random.

31. Question: Paragraph 8-304b(1). Is the contractor required to verify the citizenship of the uncleared maintenance personnel?

Answer: The contract must specify that the uncleared maintenance personnel are U.S. citizens. The ISSM may spot check the citizenship of the maintenance personnel by contacting the company if there is doubt as to the citizenship of a specific maintenance person.

32. Question: Paragraph 8-304b(3). What maintenance procedures must be identified, enforced, and documented when the IS cannot be cleared (paragraph 8-301a) either before or after maintenance?

Answer: Every effort should be made to use cleared maintenance personnel. If a cleared person is not performing maintenance, a technically knowledgeable escort is required to oversee all maintenance operations. Any, and all, vendor-supplied software used for maintenance must reside on write-protected media or be read only.

33. Question: Paragraph 8-304b(4) states that a separate copy of the operating system is used during maintenance operations. If the contractor has arranged for remote maintenance, can the original operating system that is used for classified processing stay resident on-line during the maintenance operation?

Answer: No. The contractor must use a separate copy of the operating system and any maintenance software.

34. Question: Paragraph 8-304b(4). What procedures should the ISSM implement for an IS using non-removable storage?

Answer: Same procedures identified above for paragraph 8-304b(3).

35. Question: Does DSS require external color-coded labels as per paragraph 8-306a?

Answer: No.

36. Issue: Paragraphs 8-306b and 8-310b discuss the "trusted download" process where electronic files and/or media can be created at a classification level lower than the accreditation level of the IS without going into sufficient detail of the review process or program. Because of the many different vendor platforms and applications (e.g., word processing, database, electronic mail, spreadsheets) additional guidance is needed.

Answer: Every vendor's platform and application are unique and each requires a thorough review by the ISSM and DSS before they can be used to create classified or unclassified files and/or media. DSS has developed a "standard" for the trusted download process that can be found at **www.dss.mil/infoas/index.htm.** If the ISSM is unable to implement the DSS "standard," the SSP must include a description of how and why the contractor has deviated from the standard under the vulnerability-reporting requirement of paragraph 8-610a(1)(c). If the ISSM is unable to provide any acceptable countermeasure to mitigate this vulnerability, the ISSM must notify and get acceptance from the GCA/data owner of the additional risk.

37. Issue: Paragraph 8-306c requires marking of unclassified media when classified and unclassified IS are collocated. Since the DSS approved area can range in size and structure (e.g., small office cubicle to a multi-story building) additional guidance is needed.

Answer: The purpose of externally marking media when classified and unclassified IS are collocated is to clearly convey/distinguish the classification level of the media. The ISSM/ISSO must establish well-defined perimeters for the classified IS. These perimeters not only distinguish the classified area, but assist in distinguishing classified media from unclassified media within the area. Writeable media within the classified IS area perimeter that is unmarked and not in factory sealed-packages must be considered classified and marked accordingly. Writeable media not in the classified IS area that is unmarked is considered unclassified.

38. Question: Paragraph 8-308a. How is hardware integrity maintained?

Answer: Hardware integrity of the accredited IS not processing classified information or powered off can be maintained by one or more of the following methods:

a. Continuous supervision by authorized personnel.

b. Use of approved cabinets, enclosures, seals, locks or Closed Areas.

c. Use of area controls that prevent or detect tampering or theft of the IS hardware and/or software. These controls will vary depending on the security in-depth at the contractors facility and in the immediate area of the IS.

39. Issue/Question: Paragraph 8-308b. What is the boundary of the DSS approved area.

Answer: Attended classified processing shall take place in an area where authorized contractor personnel can exercise constant surveillance and maintain control of the IS. The area shall have an identifiable boundary (e.g., walls, signs, tape on floor, rope or chains) where it is obvious that the area is restricted to only authorized personnel. Unattended classified processing requires a closed area and supplemental controls depending upon the accreditation level of the IS.

40. Question: Paragraph 8-308d. If the IS is not located in a DSS closed area, but in an office environment, does everyone in the area require a clearance or escorted?

Answer: No, provided the contractor has security-in-depth and has area controls or devices on the IS that prevent or detect tampering or theft of the IS hardware and/or software.

41. Question: Paragraph 8-310a. What software applications can be used to examine information not in human-readable form (e.g., embedded graphs, sound, video, etc)?

Answer: DSS has developed a "standard" for the trusted download process that can be found at **www.dss.mil/infoas/index.htm.** Many of the standard applications are identified and can be used with reasonable assurance that only the requested information will be transferred. However, for some applications (i.e., sound, video) there is little to no assurance in the "trusted download" process, requiring acknowledgement of the additional risk from the GCA.

42. Issue: Paragraph 8-310b indicates that DSS will approve random or representative sampling techniques when verifying large volumes of output for proper markings.

Answer: When the output is in printed form, a random sampling of no less than 20% is required. When the output is in electronic form, "text" searches or scans looking for classified information can produce the desired results.

43. Question: Paragraph 8-311. Should the CM program include peripherals as well as platforms?

Answer: Yes. Configuration Management shall be implemented on any IS component that has the capability of retaining information.

44. Question: Paragraph 8-311c. What is the Security Support Structure (SSS)?

Answer: The Security Support Structure is the hardware, software and firmware required to adjudicate security policy and implementation differences among IS components and networks. A reference guide to networks that discusses the SSS in more detail can be found at **www.dss.mil/infoas/index.htm.**

45. Question: Paragraph 8-311d(1). What is "security-relevant" hardware and software?

Answer: For hardware, any IS component that contains, or has the potential of containing, classified information. For software, all virus detection and sanitization software. Additionally, all operating system software used on an IS where Identification & Authentication is technically implemented.

46. Question: Section 4, Paragraph 8-402 does not have a protection level that corresponds to the Multilevel Security Mode. What are the security requirements for contractors who need to develop systems in the Multilevel Security Mode?

Answer: DoD has determined that the multilevel security mode is “high-risk” and should be addressed by the NISPOM Supplement. For the purposes of this ISL, systems are operating at Protection Level 4 when at least one user lacks sufficient clearance for access to all the information on the IS, but all users have at least a Confidential clearance when the IS is accredited at the Secret level or a Secret clearance when the IS is accredited at the Top Secret level.

47. Issue/Question: Section 5, Special Categories. Identifies several categories of “systems” that can be adequately secured without implementation of all the technical features and safeguards identified in Sections 3, 4 and 6. Would you clarify?

Answer: The DSS ISSP and the ISSM/ISSO develop protection measures for special categories of systems on a case-by-case basis. Once determined, the facility’s SSP will reflect the “special system” and all agreed upon protection measures.

48. Question: Paragraph 8-501. When is sanitization of memory and media required?

Answer: Sanitization of memory and media is required if the standalone system is being “released” to users with a PCL lower than the accreditation level or the standalone system is accredited at the TOP SECRET level. Clearing (paragraph 8-301a) is all that is required when changing classification levels or information sensitivity.

49. Question: Paragraph 8-502e states that the CSA shall consider manual logging for multiple user systems that are not capable of automated logging. Does DSS require manual logging, and if so, can access lists be used for validation purposes as addressed in an earlier question?

Answer: Yes. Manual logging is required, and like the answer for 8-104l, access lists can be used for validation purposes and shall be retained as an Audit 1 requirement.

50. Question: Paragraph 8-503b states that the platform on which the guard or server runs usually needs to meet no more than Protection Level 3 security requirements. Is this correct since the May Chapter 8 only has 3 Protection Levels?

Answer: Yes. The protection profile table for confidentiality (Chapter 8, Table 5) is made up of eleven requirements identifying graded requirements for the three protection levels. The wording in paragraph 8-503b does not restrict the platform on which a guard or pure server resides to a single protection level for all eleven requirements (e.g., a guard or pure server might have an access requirement of PL3 but an auditing requirement of PL1).

51. Question: Paragraph 8-500 indicates that special categories of systems do not require all the technical features and safeguards of Chapter 8 to be adequately secured. This philosophy of less applies to all systems identified in Section 5 except to guard or server applications (8-503b) where they will be provided with more stringent technical protections than the system's protection level. Please explain?

Answer: The application running on a guard or server is viewed separately from the hardware platform. It is not uncommon for the guard or pure server platform to be at a protection level less than the protection level associated with the application.

52. Question: Paragraph 8-503d. Do "pure servers" (i.e., guard, proxy server, application server) require accreditation separate from the "general-purpose computer" they support or are connected to?

Answer: Normally the only "pure server" that would require separate accreditation is a guard. The guard requires more stringent technical protection and assurance than the ISs it protects by the very nature of its function. The other types of "pure servers" can be described and included in the "general-purpose computers SSP."

53. Question: Paragraph 8-602. What security-relevant activities should be recorded for all protection levels and all special category IS?

Answer: Audit requirements 1-4 identify IS functions that are normally captured by an automated audit capability. Additionally, manual logs are required for:

a. Maintenance, repair, installation, or removal of hardware components. Log must include the component involved, the action taken and the name of the escort if the maintenance was performed by an uncleared individual.
b. Installation, testing, and modification of operating system and security-related software (if applicable). Logs must identify the software involved.
c. Periods processing times.
d. Sanitization and declassifying memory, media and devices.
e. Application and reapplication of security seals (if applicable).

54. Question: Paragraph 8-602a(1) permits an alternative method of auditing a PL-1 system when the Operating System cannot provide an automated capability. What alternative method should be used?

Answer: When the IS cannot provide an automated capability (paragraph 8-502e), or the IS meets the requirements of paragraph 8-501, manual logs are required.

55. Question: Paragraph 8-602a(1)(c) can generate upwards to 100 audit entries for each successful access to security-relevant objects and/or directories. From a security standpoint, is this information of enough importance to generate voluminous amounts of auditing data?

Answer: No. Only unsuccessful accesses need to be audited.

56. Question: How long are the audit records retained (paragraph 8-602a(4))?

Answer: Audit records covering the previous 12 months, or since the IS was accredited (which ever is less), must always be retained.

57. Question: Paragraphs 8-607b(f) requires that the IS be able to maintain a history of authenticator changes (e.g., password) with assurance of non-replication under the Audit 2 requirement. What does the contractor do if the IS is unable to meet this requirement?

Answer: The ISSM will document this as a unique vulnerability in their SSP as per paragraph 8-610a(1)(c).

58. Question: Paragraphs 8-607c requires "strong authentication" for privileged users that are either located or communicate outside the IS's perimeter. What will DSS accept for strong authentication?

Answer: Strong authentication is synonymous with cryptographic or biometric devices (e.g., one-time passwords, and retina identification).

59. Question: Paragraph 8-609b(2). What is the baseline time period of user inactivity and what procedures are required?

Answer: After 15 minutes of user inactivity, the user will be required to reauthenticate themselves (e.g., reenter password) to the IS. If it is technically not feasible for the IS to implement this requirement, or the ISSM has implemented a time period longer than 15 minutes, the ISSM will document this as a unique vulnerability in their SSP as per paragraph 8-610a(1)(c).

60. Question: Paragraph 8-614a requires the ISSM provide "assurance" where as paragraph 8-614b requires the ISSM provide "written assurance." Is there a difference and if so please explain?

Answer: The assurance the ISSM provides under Test 1 is a statement in the SSP that the security features, including access controls and configuration management, are implemented and operational. The written assurance the ISSM provides under Test 2, since technical security features and safeguards are required, is individual verification that each of the requirements of Table 5 are implemented and operational and that access controls and configuration management are implemented.

61. Question: Section 7, Paragraphs 8-700 and 8-701 refer to the use of a Controlled Interface (CI) when connecting networks of the same or different classification levels. DoD uses the term "high assurance guard." Are the terms "high assurance guard" and "controlled interface" interchangeable?

Answer: They have the same meaning but not the same depth in scope. The description of CI, as it appears in Section 7, goes beyond the definition/capability of a “high assurance guard” as it encompasses communication equipment like routers and bridges. Within DoD, the common practice is to refer to specialized equipment by the function they serve.

62. Question: Paragraph 8-700b states that a unified network must be accredited as a single entity by a single CSA. Since DSS has more than one accrediting entity, can a unified network exist which spans more than one DSS geographical region?

Answer: Yes. The DSS structure, and not its individual accreditors, is viewed as a single entity for the purpose of this requirement.

63. Question: Paragraph 8-700c indicates that an interconnected network requires accreditation as a unit. Is a network SSP required and who is responsible for it’s preparation?

Answer: Yes. Normally the prime contractor or one of its sub-contractors prepares the network SSP. Additionally, a network ISSO must be assigned whose job is to oversee the security of the network.

64. Issue/Question: Paragraph 8-700d states that interconnected systems (i.e., networks) can process information at different classification levels or different compartments What are the required technical security features, safeguards and assurances?

Answer: Since the purpose of the CI is to provide protection to IS at different classification levels or compartments, the CI will have to have been evaluated and found to meet the B3 level of trust under the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) program, or the EAL6 level under the Common Criteria.

65. Question: As a follow on to the above question, when a contractor has a connection to a government network and has a CI that is used to transfer information of a different classification level, what security features, safeguards and assurances are required?

Answer: DoD requires that the contractor use a CI evaluated and certified under DoD’s Secret and Below Interoperability (SABI) program. A list of evaluated SABI products is posted at **www.dss.mil/infoas/index.htm** along with requirements for certification and accreditation.

66. Question: Must the contractor use a CI from the SABI program when networks belonging only to contractors are interconnected at different classification levels or different compartments?

Answer: No. However, the CI must be of an equivalent evaluation as the CI from the SABI program.

67. Question: What requirements of the new chapter 8 apply to both Restricted FGI and NATO information?

Answer: Generally, the requirements of the new Chapter 8 apply but to a lesser standard as they would for U.S. Confidential, Secret or Top Secret information:

a. Accredited to the Restricted level (Section 2, NISPOM).

b. Users do not require a clearance except when Spanish Restricted information is resident (ISL 95L-2).

c. Sanitization of memory and media can be accomplished by following the "clearing" procedures identified in the clearing and sanitization matrix at **www.dss.mil/infoas/index.htm.**

d. Physical security to the IS to include all components will be one or a combination of the following:

1. Secured in areas protected by key operated locks (5 pin tumbler locks) constructed in a manner which precludes surreptitious access.
2. Equipment protected with seals in an area that has been identified as having security in-depth. If the restricted information remains resident on the IS during periods of non-use, the IS must be accredited to meet the PL2 Confidentiality requirements.

e. Data transmission (paragraph 8-605a(1)(b)) within the contractor's facility (i.e., local area network) must be encrypted using an encryption key of at least 128 bits (i.e., Data Encryption Standard (DES) or Public key/Private key products of a good commercial grade).

f. Data transmission (Section 7) that leaves the contractor's facility (i.e., interconnected or unified network) must use the encryption device specified by the foreign government.

g. IS that process Restricted information can be connected to unclassified IS or networks provided they are connected through a Controlled Interface (paragraphs 8-701 and 8-702).

h. All other requirements of the May 1st Chapter 8 apply.